Privacy Impact Assessment (PIA) for MEDFAR MYLE Platform

Before you start

- This Privacy Impact Assessment (PIA) form is used by VCC to assess whether a new initiative, or proposed significant change to an existing initiative, meets the privacy protection requirements of the B.C. *Freedom of Information and Protection of Privacy Act.* FIPPA's protection of privacy requirements. A PIA is a legislative requirement (FIPPA s. 69(5.3)) and mandatory before implementing an initiative.
- You/Your refers to the individual responsible for drafting this PIA, who should be an individual from the relevant department or program area with sufficient knowledge to do so. The PIA must be signed by the role within the program area with the appropriate position to hold accountability for this initiative.
- Please include references to other documents when applicable, but do not insert or embed any documents to/in this assessment form.

- Please review the initial assessment questions and contact the Privacy Office at privacyandfoi@vcc.ca before you begin the form, if you have not already. See more guidance about the PIA process, including the supplementary Guidance Document, on the myVCC Privacy website.

PART 1: GENERAL INFORMATION

PIA file number: #2025-004

Initiative title:	MEDFAR MYLE Integrated Care Platform for MOA Program
VCC Department / Program Area:	Applied Business Department
Link to VCC initiative website:	N/A
Link to vendor website:	https://www.medfarsolutions.com/en/
Link to vendor privacy policy:	N/A
Your name and title:	Julia Slade, Dept Head, Applied Business Department
Your work phone and email:	jslade@vcc.ca 604 443 8525
Initiative Lead name and title:	Julia Slade, Dept Head, Applied Business Department
Initiative Lead phone and email:	jslade@vcc.ca 604 443 8525

General information about the PIA:

Is this initiative a data-linking program under FIPPA? See the definition in Schedule 1 of FIPPA. If this PIA addresses a data-linking program, the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No
Is this initiative a common or integrated program or activity? See the definition of Schedule 1 of FIPPA. Under section FIPPA 69 (5.4), the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No
Does this initiative involve a regular or systematic exchange of personal information between organizations? If yes, this initiative may require an Information Sharing Agreement.	No
Related PIAs, if any:	

1. What is the initiative?

MYLE Integrated Care Platform, by MEDFAR Clinical Solutions, is a cloud-based electronic medical records system and platform used for administration in medical offices. VCC's Applied Business Department is obtaining this software for use by Medical Office Administration students to learn, practice, and be assessed on MOA skills, including:

- Scheduling for patients, staff, and doctors (adding, removing, or changing appointments)
- Maintaining the daily time sheet accurately
- Adding notes and reminders to staff and doctors' pages
- Changing demographic and geographical data in patient records
- Write and submit consult letters from doctors, nurse practitioners, and other allied health professionals
- Submit completed test results into records and flag doctors to review
- Practice MSP billing
- Provide approved educational resources and materials for patients

All patient data will be fictional and for training purposes; the initiative will only involve student's personal information through creation of accounts (using an identifier assigned to them by the Instructor and known only to the Instructor) and the work that they produce during courses while utilizing the software. The Instructor who takes the role of Clinic Manager has the ability to view and assess the MOA students' work in the department's constructed clinic. s. 21(1)

2. What is the scope of the PIA?

This PIA covers the collection, use, and disclosure of students' and instructors' personal information involved in the practical/training use of MYLE EMR system in the MOA program only.

3. What are the data or information elements involved in your initiative?

Instructor:

- Name, work email, and employee ID for account creation.
- Collected directly from instructor and used to create an account as "Clinical Manager" that oversees the entire clinic.

Students:

- Students working in the clinic as MOAs are assigned an account within MYLE (e.g. MOA1, MOA2, etc.) by the Instructor. The Instructor will hold the master sheet of generic accounts linked to student names/ID numbers within the class, which is obtained from the class list.
- Generic accounts are cleared at the end of each cohort's time in the clinic.
- Students are assessed on their work within MYLE associated with their assigned MOA account.

Patients: All patient data is not real and is created by instructors to simulate realistic patient scenarios, workplace demands, scheduling, staff communication etc.

3.1 Did you list personal information in question 3?

Yes (employee ID number; account ID associated with student; student's educational history – assignments/work within MYLE).

- If yes, are all of the personal information elements **necessary** for your initiative?
    - Yes: Instructors and students must create accounts in order to use the system and practice MOA skills.

4. If you answered "no" to question 3.1: How will VCC reduce the risk of unintentionally collecting personal information?

N/A

PART 2: COLLECTION, USE, AND DISCLOSURE

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use, and disclosure flow

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FIPPA authority or other legal authority	Specify any potential risks
Instructors create account with name, VCC email, and employee ID number for Instructor access to MYLE.	Collection	26(c)	
Instructors create generic accounts (username and password) and assign them to MOA students within the active cohort for access to MYLE. Instructors use a master list to associate identifiers (e.g. MOA1, MOA2...) with the students in class (name, student ID); the link between student and identifier is only known by instructors, but each account is unique to 1 student.	Collection Use	26(c) 32(a)	
Students use MYLE in the course of their learning activities in the constructed clinic, using simulated patient data, and only using their unique assigned account.	Use Collection	32(a) 26(c)	
Instructor/Clinic Manager with licence reviews all students' use of MYLE for coursework and assesses students' work. Instructor may assess or give grades for student's own learning and records.	Use	32(a)	
Department deletes all of students' information at the end of each course in preparation of the next cohort. Gradebooks are retained according to retention schedule.	Disposal	31	Deletion of coursework: Students are informed that they may retain copies/screenshots of their assignments in MYLE for their records.

6. Collection Notice and Consent

6. 1 Collection Notice

If you are collecting personal information directly from an individual the information is about, FIPPA s. 27(2) requires that you provide a collection notice (except in limited circumstances). If your vendor is collecting personal information on behalf of VCC, the vendor must also provide a collection notice. FIPPA requires that you notify the individual of:

- *the legal authority,*
- *purpose(s) and use of their personal information (including any third party disclosures), and*
- *contact information or someone who can answer questions about the collection and use.*

When you use the MEDFAR MYLE platform, your personal information is collected under the authority of section 26(c) of the BC *Freedom of Information and Protection of Privacy Act* (FIPPA). This information will be used for creating your account (by assigning you a unique account) and sharing your activity with your instructor and in order for you to complete required coursework. Questions about the collection and use of this information may be directed to [Julia Slade, Department Head, jslade@vcc.ca] or you may speak with your instructor.

*(Instructor assigned at beginning of each cohort)

The collection notice will be posted in the students' list of required materials or syllabus. In addition, instructors will talk about the MYLE platform with students on the first day of their clinic and can further explain how users' data will be used and protected. Department and Instructor also have access to the platform support team. Students are also encouraged to manage and save their own file pathways in the event of technology malfunctions and will be instructed to retain copies/screenshots of their work as assignments if needed after the course.

6. 2 Consent

N/A

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

No: MEDFAR MYLE EMR system only stores and accesses personal information in Canada.

8. **If you answered yes to Question 7: Where are you storing the personal information involved in your initiative?**

N/A

9. **Does your initiative involve sensitive personal information that will be stored outside of Canada?**

N/A

- If yes, go to question 10
- If no, skip ahead to Part 5

10. **If you answered "yes" to Question 9: Is the sensitive personal information being stored outside of Canada only because it is being made available to the public under an enactment that authorizes or requires the information to be made public (FIPPA section 33(2)(f))?**

N/A

- If yes, what enactment?
    - [Answer] then skip ahead to Part 5.
- If no, go to Part 4.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section **only if you answered yes to Question 9: you are disclosing sensitive personal information to be stored outside of Canada**. This section will require consultation with a representative from IT Services.

11. **Is the sensitive personal information stored by a service provider?**

N/A

- If yes, fill in the table below (add more rows if necessary) and then go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

12. If you answered "no" to Question 11: Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

N/A

13. Does the contract you rely on include privacy-related terms?

N/A

- If yes, describe the contractual measures related to your initiative.
  - **N/A**
- Is VCC's Privacy Protection Schedule or Privacy Protection Schedule for Cloud Services appended to the initiative's contract? **N/A**

14. What controls are in place to prevent unauthorized access to sensitive personal information?

N/A

15. Provide details about how you and will track access to sensitive personal information.

N/A

16. Describe the privacy risks for disclosure outside of Canada.

Privacy risk	Impact to individuals (low, medium, high)	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Outcome of Part 4

The outcome of Part 4 will be a risk-based decision made by the role designated accountable for the initiative on whether to proceed with the initiative, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 16.

Is the outcome to proceed with the initiative? [Answer: Yes or No]

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5, you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You and/or your vendor need to make sure that the personal information is safely secured in both physical and technical environments.

17. Does your initiative involve digital tools, databases, or information systems?

Yes

- If yes: Are these digital tools, databases, or information systems new to VCC?
  - Yes.

17.1 If you answered "yes" to Question 17: Do you or will you have a security assessment to ensure the initiative meets the security requirements of FIPPA s. 30?

Consult with VCC IT Services to complete a security assessment that will ensure that the initiative has reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or disposal of personal information.

Yes.

- If yes, go to question 19. If you have or will complete a security assessment during the development of your initiative, you do not need to answer the question about technical security.

- If no, continue to question 18.

18. What technical and physical security do you have in place to protect personal information?

IT Services is completing a security assessment. The Applied Business Department will create accounts specific to instructors and use role-based access (for students in the clinic, and for instructors with admin access).

19. Controlling and tracking access

Strategy	
We only allow employees in certain roles access to information:	Yes
Employees that need standing or recurring access to personal information must be approved by their managerial lead:	Yes
We use audit logs to see who accesses a file and when:	Yes
Describe any additional controls:	s. 15(1)(l), s. 21(1) [redacted]

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6, you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

20. How will you make sure that the personal information is accurate and complete?

- Instructors create their accounts directly and can review their personal information for accuracy and completeness at that time. Instructors assign generic account identifiers (MOA1, MOA2, etc.) to class list, linked to each student's name and student ID number, to ensure accuracy.
- Students directly contribute to the MYLE platform during their time in the clinic (assignments they may be assessed or graded on) and have the opportunity to review for accuracy and completeness before submitting.
- Students maintain and save work to their file-folder pathways for verification of work in the event of accidental deletion or technology malfunction.

21. Requests for correction

21.1 Do you have a process in place to correct personal information?

Yes.

- If yes: Please describe the process.
    - Students may directly contact their Instructor to correct any PI associated with their account/work in MYLE. Instructors may correct their own.

21.2 Sometimes it's not possible to correct the personal information. FIPPA s. 29 requires that you make a note on the record about the request for correction if you are not able to correct the record itself. Will you document the request to correct or annotate the record?

Yes: Instructors may make a note in students' records if something cannot be corrected in MYLE.

21.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FIPPA s. 29 requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A - No personal information from this initiative will be disclosed to another public body or third party.

22. Does your initiative use personal information to make decisions that directly affect an individual?

Yes: Students are assessed on their contributions to the MEDFAR MYLE platform as part of coursework.

- If yes, go to question 23

23. If you answered "yes" to Question 22: Do you have a records retention schedule in place related to personal information used to make a decision?

FIPPA s. 31 requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. Please consult the VCC Records Retention Schedule to assist you in answering this question.

Yes - per TE 400 classification in VCC Records Retention Schedule and Moodle LifeCycle Policy

Instructor retains the gradebook per TE 400 retention policy. Students are responsible for keeping a copy of their contributions to MYLE (through copying or screenshots). At the end of a course, students' work within MYLE is deleted and generic MYLE accounts are cleaned up and reset for the next cohort.

PART 7: PERSONAL INFORMATION BANKS

24. Will your initiative result in a personal information bank?

No.

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

25. Risk response

N/A - No additional risks identified.

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to the Privacy Office for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

This PIA only considers the teaching & learning use of MYLE in VCC's constructed clinic. This PIA must be revised if any other collection of student information occurs (e.g. creating non-generic accounts for students) or if this system is ever used for actual patient data and records. This PIA does not approve the use of the system for any use other than teaching and learning in the Applied Business Department.

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer	Caralee Maloney	Caralee Maloney Digitally signed by Caralee Maloney Date: 2025.03.14 15:10:43 -07'00'	March 14, 2025

Program Area Signatures

The PIA must be signed by a role that is able to hold accountability for a PIA, proportionate to the sensitivity of personal information and/or the risks of the initiative. This signature confirms that this PIA accurately documents data elements and information flow at the time of signing. If there are any changes to the overall initiative, including the way personal information is collected, used, stored, or disclosed, the program area will contact Privacy and, if necessary, complete a PIA update.

Program Area Comments:

Role	Name/Position	Electronic signature	Date signed
Role designated accountable for the initiative	Julia Slade-DH	Julia Slade Digitally signed by Julia Slade Date: 2025.03.17 13:12:53 -07'00'	March 17, 2025
Contact Responsible for Systems Maintenance and/or Security	Norman Chang	Norman Chang Digitally signed by Norman Chang Date: 2025.03.14 14:46:31 -07'00'	March 14, 2025